

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-281012

(P2002-281012A)

(43) 公開日 平成14年9月27日 (2002.9.27)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
H 0 4 L 9/08		G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
G 0 6 F 15/00	3 3 0	H 0 4 L 9/00	6 0 1 D 5 J 1 0 4
H 0 4 L 9/32			6 0 1 C
			6 7 3 B

審査請求 未請求 請求項の数11 O L (全 13 頁)

(21) 出願番号 特願2001-81245(P2001-81245)

(22) 出願日 平成13年3月21日 (2001.3.21)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 吉田 和弘

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(72) 発明者 田村 聡

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74) 代理人 100077849

弁理士 須山 佐一

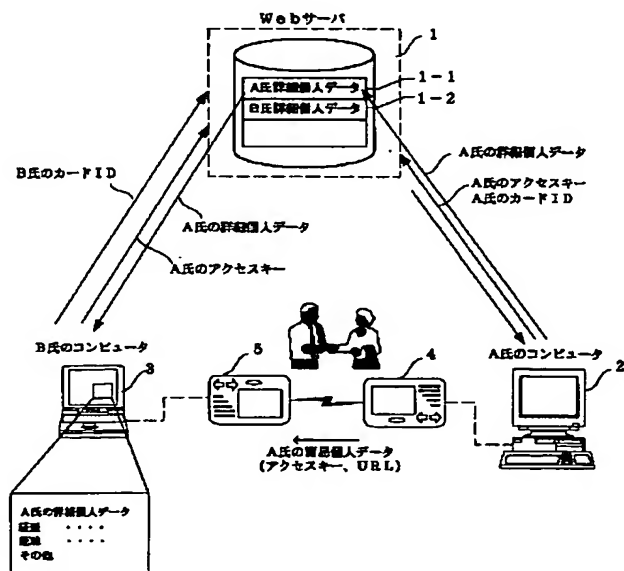
最終頁に続く

(54) 【発明の名称】 データ交換システム、データ交換方法、カード型無線端末、パスワード処理方法およびカード型パスワード処理装置

(57) 【要約】

【課題】 インターネットを用いたデータの交換において、面識の無いデータ交換相手とのデータ交換を制限してセキュリティの向上を図る。

【解決手段】 Webサーバ1にアクセスキーで暗号化した詳細個人データを配置しておき、詳細個人データを公開したい相手に、カード型無線端末4、5を使ってアクセスキーを無線で提供する。アクセスキーを入手した利用者はコンピュータを使ってアクセスキーをWebサーバ1に転送する。この結果、Webサーバ1はそのアクセスキーで詳細個人データの暗号を解除して利用者に配信する。また、Webサーバ1上の詳細個人データに再配信防止の属性を付与すれば、その詳細個人データは配信要求元の利用者のカード型無線端末のカードIDによってデータを暗号化して配信する。



1

【特許請求の範囲】

【請求項 1】 それぞれ異なる利用者によって利用される複数のカード型無線端末と、それぞれ個々の前記カード型無線端末と接続される複数のコンピュータと、前記各コンピュータとインターネットを通じて接続されるサーバとを備え、

前記各カード型無線端末がそれぞれ、少なくとも所定のアクセスキーが記憶された記憶部と、この記憶部に記憶された前記アクセスキーをデータ交換相手である利用者の前記カード型無線端末との間で無線でやりとりする無線通信部と、この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、前記コンピュータとのインタフェース部とを有し、前記サーバが、前記各利用者の交換対象データが格納されるデータ格納スペースと、一方の利用者の前記コンピュータよりインターネットを通じて転送された交換対象データを該一方の利用者の前記カード型無線端末の前記記憶部に記憶された前記アクセスキーで暗号化して前記データ格納スペースに格納する機能と、他方の利用者の前記コンピュータよりインターネットを通じて転送された、該他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、かつ復号された交換対象データを前記他方の利用者の前記コンピュータへ配信する配信機能とを有することを特徴とするデータ交換システム。

【請求項 2】 それぞれ異なる利用者によって利用される複数のカード型無線端末と、それぞれ個々の前記カード型無線端末と接続される複数のコンピュータと、前記各コンピュータとインターネットを通じて接続されるサーバとを備え、

前記各カード型無線端末がそれぞれ、少なくともカード ID および所定のアクセスキーが記憶された記憶部と、この記憶部に記憶された前記アクセスキーをデータ交換相手である利用者の前記カード型無線端末との間で無線でやりとりする無線通信部と、この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、前記コンピュータとのインタフェース部とを有し、

前記サーバが、前記各利用者の交換対象データが格納されるデータ格納スペースと、一方の利用者の前記コンピュータよりインターネットを通じて転送された交換対象データを前記一方の利用者の前記カード型無線端末の前記記憶部に記憶された前記アクセスキーで暗号化して前記データ格納スペースに格納する機能と、他方の利用者の前記コンピュータよりインターネットを通じて転送された、該他方の利用者の前記カード型無線端末の前記記

2

憶部に登録された前記外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、かつ復号された交換対象データを前記他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記カード ID により暗号化して前記他方の利用者の前記コンピュータへ配信する配信機能とを有し、かつ前記各カード型無線端末がそれぞれ、前記サーバより配信された交換対象データを前記記憶部に記憶された前記カード ID で復号する機能をさらに有することを特徴とするデータ交換システム。

【請求項 3】 それぞれ異なる利用者によって利用される複数のカード型無線端末と、それぞれ個々の前記カード型無線端末と接続される複数のコンピュータと、前記各コンピュータとインターネットを通じて接続されるサーバとを備え、

前記各カード型無線端末がそれぞれ、少なくともカード ID および所定の複数のアクセスキーが記憶された記憶部と、この記憶部に記憶された前記複数のアクセスキーのうちのの一つを選択してデータ交換相手である利用者の前記カード型無線端末との間で無線でやりとりする無線通信部と、この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、前記コンピュータとのインタフェース部とを有し、前記サーバが、前記各利用者の交換対象データが格納されるデータ格納スペースと、一方の利用者の前記コンピュータよりインターネットを通じて転送された個々の交換対象データを前記一方の利用者の前記カード型無線端末の前記記憶部に記憶された個々の前記アクセスキーで各々暗号化して前記データ格納スペースに格納する機能と、他方の利用者の前記コンピュータよりインターネットを通じて転送された、該他方の利用者の前記カード型無線端末の前記記憶部に登録された前記外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、かつ復号された交換対象データを前記他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記カード ID により暗号化して該他方の利用者の前記コンピュータへ配信する配信機能とを有し、かつ前記カード型無線端末がそれぞれ、前記サーバより配信された交換対象データを前記記憶部に記憶された前記カード ID で復号する機能をさらに有することを特徴とするデータ交換システム。

【請求項 4】 それぞれ異なる利用者ごとに用意された複数のカード型無線端末の記憶部に少なくとも所定のアクセスキーを記憶しておき、一方の利用者の前記カード型無線端末の前記記憶部に記憶された前記アクセスキーをデータ交換相手である他方の利用者のカード型無線端末へ無線で転送してこのカード型無線端末の記憶部に外

3

部アクセスキーとして登録する段階と、
 一方の利用者の前記カード型無線端末に接続されたコンピュータをインターネットを通じてサーバに接続し、前記コンピュータから前記サーバへ交換対象データならびに前記カード型無線端末の前記記憶部に記憶されたアクセスキーをそれぞれ転送する段階と、
 前記サーバに前記各利用者の交換対象データが格納されるデータ格納スペースを設けておき、このサーバにて、前記コンピュータから転送された交換対象データを同じく前記コンピュータから取得したアクセスキーで暗号化して前記データ格納スペースに格納する段階と、
 前記他方の利用者の前記カード型無線端末に接続されたコンピュータから前記サーバへ前記カード型無線端末の前記記憶部に記憶された外部アクセスキーを転送する段階と、
 前記サーバにて、所得した外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、復号データを前記他方の利用者の前記コンピュータへ配信する段階と
 を有することを特徴とするデータ交換方法。

【請求項5】 それぞれ異なる利用者ごとに用意された複数のカード型無線端末の記憶部に少なくともカードIDおよび所定のアクセスキーを記憶しておき、一方の利用者の前記カード型無線端末の前記記憶部に記憶された前記アクセスキーをデータ交換相手である他方の利用者のカード型無線端末へ無線で転送してこのカード型無線端末の記憶部に外部アクセスキーとして登録する段階と、
 一方の利用者の前記カード型無線端末に接続されたコンピュータをインターネットを通じてサーバに接続し、前記コンピュータから前記サーバへ交換対象データならびに前記カード型無線端末の前記記憶部に記憶されたアクセスキーをそれぞれ転送する段階と、
 前記サーバに前記各利用者の交換対象データが格納されるデータ格納スペースを設けておき、このサーバにて、前記コンピュータから転送された交換対象データを同じく前記コンピュータから取得したアクセスキーで暗号化して前記データ格納スペースに格納する段階と、
 前記他方の利用者の前記カード型無線端末に接続されたコンピュータから前記サーバへ前記カード型無線端末の前記記憶部に記憶された外部アクセスキーを転送する段階と、
 前記サーバにて、取得した外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、この復号データを前記他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記カードIDにより暗号化して該他方の利用者の前記コンピュータへ配信する段階と、

(3)

特開2002-281012

4

前記他方の利用者の前記カード型無線端末にて、前記サーバから前記他方の利用者の前記コンピュータへ配信された交換対象データを取得し、前記他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記カードIDで復号する段階とを有することを特徴とするデータ交換方法。

【請求項6】 それぞれ異なる利用者ごとに用意された複数のカード型無線端末の記憶部に少なくともカードIDおよび所定の複数のアクセスキーを記憶しておき、一方の利用者の前記カード型無線端末の前記記憶部に記憶された前記複数のアクセスキーのうちの一つを選択してデータ交換相手である他方の利用者のカード型無線端末へ無線で送信してこのカード型無線端末の記憶部に外部アクセスキーとして登録する段階と、
 一方の利用者の前記カード型無線端末に接続されたコンピュータをインターネットを通じてサーバに接続し、前記コンピュータから前記サーバへ個々の交換対象データならびに前記カード型無線端末の前記記憶部に記憶された個々のアクセスキーをそれぞれ転送する段階と、
 前記サーバに前記各利用者の交換対象データが格納されるデータ格納スペースを設けておき、このサーバにて、前記コンピュータから転送された個々の交換対象データを同じく前記コンピュータから取得した個々のアクセスキーでそれぞれ暗号化して前記データ格納スペースに格納する段階と、
 前記他方の利用者の前記カード型無線端末に接続されたコンピュータから前記サーバへ前記カード型無線端末の前記記憶部に記憶された外部アクセスキーを転送する段階と、
 前記サーバにて、取得した外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、この復号データを前記他方の利用者の前記カード型無線端末の前記記憶部に記憶されたカードIDにより暗号化して該他方の利用者の前記コンピュータへ配信する段階と、
 前記他方の利用者の前記カード型無線端末にて、前記サーバより前記他方の利用者の前記コンピュータへ配信された交換対象データを取得し、前記他方の利用者の前記カード型無線端末の前記記憶部に記憶されたカードIDで復号する段階とを有することを特徴とするデータ交換方法。

【請求項7】 少なくとも所定のアクセスキーが記憶された記憶部と、
 この記憶部に記憶された前記アクセスキーを他のカード型無線端末との間で無線でやりとりする無線通信部と、
 この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、
 複数の利用者の交換対象データが格納されるデータ格納

5

スペースを有するサーバとインターネットを通じて接続されたコンピュータとのインタフェース部と、前記コンピュータから前記サーバへの交換対象データの転送に伴い、この交換対象データが前記記憶部に記憶されたアクセスキーで暗号化されて前記サーバのデータ格納スペースに格納されるように、前記記憶部に記憶されたアクセスキーを前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させるアクセスキー転送手段と、

前記サーバのデータ格納スペースから他の利用者の暗号化された交換対象データをアクセスして暗号化を解除するために、前記記憶部に記憶された外部アクセスキーを前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させる外部アクセスキー転送手段と、

を具備することを特徴とするカード型無線端末。

【請求項 8】 少なくともカード ID および所定のアクセスキーが記憶された記憶部と、

この記憶部に記憶された前記アクセスキーを他のカード型無線端末との間で無線でやりとりする無線通信部と、この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、複数の利用者の交換対象データが格納されるデータ格納スペースを有するサーバとインターネットを通じて接続されたコンピュータとのインタフェース部と、

前記コンピュータから前記サーバへの交換対象データの転送に伴い、この交換対象データが前記記憶部に記憶されたアクセスキーで暗号化されて前記サーバのデータ格納スペースに格納されるように、前記記憶部に記憶されたアクセスキーを前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させるアクセスキー転送手段と、

前記サーバのデータ格納スペースから他の利用者の暗号化された交換対象データをアクセスして暗号化を解除するために、前記記憶部に記憶された外部アクセスキーを前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させる外部アクセスキー転送手段と、

前記外部アクセスキーによって暗号化が解除された交換対象データが前記記憶部に記憶された前記カード ID で暗号化されて前記コンピュータへ配信されるように、前記記憶部に記憶された前記カード ID を前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させるカード ID 転送手段と、

前記カード ID で暗号化されて前記コンピュータへ配信された交換対象データを取得し、前記記憶部に記憶された前記カード ID で復号する復号手段とを具備することを特徴とするカード型無線端末。

6

【請求項 9】 少なくともカード ID および所定の複数のアクセスキーが記憶された記憶部と、

この記憶部に記憶された前記複数のアクセスキーのうちの一つを選択して他のカード型無線端末との間で無線でやりとりする無線通信部と、

この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、

複数の利用者の交換対象データが格納されるデータ格納スペースを有するサーバとインターネットを通じて接続されたコンピュータとのインタフェース部と、

前記コンピュータから前記サーバへの個々の交換対象データの転送に伴い、これらの交換対象データが前記記憶部に記憶された個々のアクセスキーでそれぞれ暗号化されて前記サーバのデータ格納スペースに格納されるように、前記記憶部に記憶された前記複数のアクセスキーを前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させるアクセスキー転送手段と、

前記サーバのデータ格納スペースから他の利用者の暗号化された交換対象データをアクセスして暗号化を解除するために、前記記憶部に記憶された外部アクセスキーを前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させる外部アクセスキー転送手段と、

前記外部アクセスキーによって暗号化が解除された交換対象データが前記記憶部に記憶された前記カード ID で暗号化されて前記コンピュータへ配信されるように、前記記憶部に記憶された前記カード ID を前記インタフェース部を通じて前記コンピュータへ転送し、前記コンピュータから前記サーバへ転送させるカード ID 転送手段と、

前記カード ID で暗号化されて前記コンピュータへ配信された交換対象データを取得し、前記記憶部に記憶された前記カード ID で復号する復号手段とを具備することを特徴とするカード型無線端末。

【請求項 10】 少なくともカード ID を記憶する記憶部と、この記憶部に記憶されたカード ID で暗号化データを復号する復号部と、コンピュータとのインタフェース部とを備えたカード型パスワード記憶装置をコンピュータに接続しておくとともに、前記コンピュータをこのコンピュータ上で動作されるソフトウェアの使用制限を解除するためのパスワードの提供元であるサーバとインターネットを通じて接続しておき、前記コンピュータは前記サーバに前記カード型パスワード記憶装置の前記記憶部に記憶されたカード ID を転送し、前記サーバは前記コンピュータから転送されたカード ID で前記パスワードを暗号化して前記コンピュータに送信し、前記カード型パスワード記憶装置は前記コンピュータ経由で前記暗号化されたパスワードを所得して前記記憶部に登録

7

し、前記コンピュータ上で前記ソフトウェアが起動される度に、前記記憶した暗号化パスワードを前記記憶部に記憶されたカードIDで復号して前記コンピュータへ転送することを特徴とするパスワード処理方法。

【請求項11】 少なくともカードIDが記憶された記憶部と、

ソフトウェアの使用制限を解除するためのパスワードの提供元であるサーバとインターネットを通じて接続されたコンピュータとのインタフェース部と、

前記記憶部に記憶されたカードIDを前記インタフェース部を通じて前記コンピュータに転送するカードID送信手段と、

前記コンピュータから前記サーバに前記カードIDが転送された後、前記サーバによって前記カードIDで暗号化され、前記コンピュータに転送されたパスワードを前記インタフェース部を通じて取得し、前記記憶部に登録するパスワード登録手段と、

前記コンピュータ上で前記ソフトウェアが起動される度に、前記記憶部に登録されたパスワードを前記記憶部に記憶されたカードIDで復号して前記コンピュータへ転送するパスワード転送手段とを具備することを特徴とするカード型パスワード処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネットを用いて個人データなどの交換を行うデータ交換システム、データ交換方法およびカード型無線端末に関する。また、本発明は、著作権情報の使用許可を得るためのパスワードを管理するパスワード管理機器およびパスワード管理方法に関するものである。

【0002】

【従来の技術】機密性をもつ情報たとえば個人データなどの交換には、たとえば名刺のような紙ベースの媒体が用いられてきたが、近年インターネットを利用するために必要な通信インフラの整備が進み、個人データを交換する手段としてインターネットが利用される例が増してきている。

【0003】たとえば、個人データを記述したHTMLファイル等をWebサーバに配置しておき、そのURLを公開相手に通知し、公開相手はそのURLを使って目的のHTMLファイルを読み出し、WWWブラウザを通してコンピュータ上で閲覧することができる。

【0004】この場合、Webサーバ上に配置した個人データへのアクセスにパスワードなどによる制限を設けたり、データを暗号化して転送することによって個人データの漏洩防止を図ることが可能である。

【0005】

【発明が解決しようとする課題】インターネットを用いた従来のデータ交換方式では、個人データなどのデータをWebで公開している本人の知らないところでURL

(5)

特開2002-281012

8

やパスワードがやりとりされることで、本人には面識されない者にまでデータを公開してしまい、本人にとって不利益を生む場合がある。

【0006】また、デジタルデータは制限なく複製が作れてしまうことから、パスワード等によるアクセス制限や転送データの暗号化によってデータの一次流出は避けられたとしても、公開を許されている者が一旦ダウンロードしたデータの再配信までは防止しようがない。

【0007】さらに、本発明の解決しようとする課題は以下に及ぶ。ビデオ、音楽、ゲーム、アプリケーションプログラムといった有償のソフトウェアに何らかの機能的な制限を設けておき、ユーザがソフトウェア提供者との間で使用契約を結んだところで、そのユーザに制限解除のためのパスワードを通知してソフトウェアの使用を許可するといった仕組みが、ソフトウェアの一般的な配布方法として存在する。しかし、この方法では、パスワードをユーザごとに異なるように設定することは現実的に困難であり、このためパスワードの流用等による有償ソフトウェアが不正に使用される場合が発生していた。

【0008】本発明はこのような課題を解決するためのもので、インターネットを用いたデータの交換において、面識の無いデータ交換相手とのデータ交換を制限してセキュリティの向上を図ることのできるデータ交換システム、データ交換方法およびカード型無線端末の提供を目的とする。

【0009】また、本発明は、インターネットを用いたデータの交換において交換対象データの再配信による漏洩を防止してセキュリティの強化を図ることのできるデータ交換システム、データ交換方法およびカード型無線端末の提供を目的とする。

【0010】さらに、本発明は、パスワードの流用による不正なソフトウェア使用を防止することのできるパスワード処理方法およびカード型パスワード処理装置の提供を目的とする。

【0011】

【課題を解決するための手段】上記の目的を達成するために、第1の発明のデータ交換システムは、それぞれ異なる利用者によって利用される複数のカード型無線端末と、それぞれ個々の前記カード型無線端末と接続される複数のコンピュータと、前記各コンピュータとインターネットを通じて接続されるサーバとを備え、前記各カード型無線端末がそれぞれ、少なくとも所定のアクセスキーが記憶された記憶部と、この記憶部に記憶された前記アクセスキーをデータ交換相手である利用者の前記カード型無線端末との間で無線でやりとりする無線通信部と、この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、前記コンピュータとのインタフェース部とを有し、前記サーバが、前記各利用者の交換対象データが格納されるデー

タ格納スペースと、一方の利用者の前記コンピュータよりインターネットを通じて転送された交換対象データを該一方の利用者の前記カード型無線端末の前記記憶部に記憶された前記アクセスキーで暗号化して前記データ格納スペースに格納する機能と、他方の利用者の前記コンピュータよりインターネットを通じて転送された、該他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、かつ復号された交換対象データを前記他方の利用者の前記コンピュータへ配信する配信機能とを有することを特徴とする。

【0012】すなわち、本発明では、データを提供する側の利用者のカード型無線端末のアクセスキーがデータの配信を受ける側の利用者のカード型無線端末へ無線で転送される。配信を受ける側の利用者は、このデータを提供する側の利用者よりもらい受けたアクセスキーを使ってサーバに置かれた交換対象データにアクセスする。サーバのデータ格納スペースから取り出された交換対象データは前記アクセスキーを使って暗号化が解除され、配信を受ける側の利用者へ配信される。

【0013】このように本発明によれば、配信を受ける側の利用者は、データを提供する側の利用者のカード型無線端末からアクセスキーをもらい受けてはじめて交換対象データの配信を受けることが可能となるので、データを交換する当事者どうしが直接面会したことを条件としたデータ交換が可能となり、セキュリティの向上を図ることができる。

【0014】また、第2の発明のデータ交換システムは、それぞれ異なる利用者によって利用される複数のカード型無線端末と、それぞれ個々の前記カード型無線端末と接続される複数のコンピュータと、前記各コンピュータとインターネットを通じて接続されるサーバとを備え、前記各カード型無線端末がそれぞれ、少なくともカードIDおよび所定のアクセスキーが記憶された記憶部と、この記憶部に記憶された前記アクセスキーをデータ交換相手である利用者の前記カード型無線端末との間で無線でやりとりする無線通信部と、この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、前記コンピュータとのインタフェース部とを有し、前記サーバが、前記各利用者の交換対象データが格納されるデータ格納スペースと、一方の利用者の前記コンピュータよりインターネットを通じて転送された交換対象データを前記一方の利用者の前記カード型無線端末の前記記憶部に記憶された前記アクセスキーで暗号化して前記データ格納スペースに格納する機能と、他方の利用者の前記コンピュータよりインターネットを通じて転送された、該他方の利用者の前記カード型無線端末の前記記憶部に登録された前記外部アクセ

スキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、かつ復号された交換対象データを前記他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記カードIDにより暗号化して前記他方の利用者の前記コンピュータへ配信する配信機能とを有し、かつ前記各カード型無線端末がそれぞれ、前記サーバより配信された交換対象データを前記記憶部に記憶された前記カードIDで復号する機能をさらに有することを特徴とする。

【0015】すなわち、この発明では、前記第1の発明によって得られる作用効果とともに、サーバから配信先のコンピュータへ、交換対象データが当該配信先の利用者のカード型無線端末のカードIDによって暗号化されて配信されるので、仮に配信先のコンピュータから交換対象データが外部へ再配信されたとしても、再配信先では前記カードIDによる暗号化データを復号して中身を参照することはできない。したがって、個人データの漏洩を防止でき、セキュリティを強化できる。

【0016】さらに、第3の発明のデータ交換システムは、それぞれ異なる利用者によって利用される複数のカード型無線端末と、それぞれ個々の前記カード型無線端末と接続される複数のコンピュータと、前記各コンピュータとインターネットを通じて接続されるサーバとを備え、前記各カード型無線端末がそれぞれ、少なくともカードIDおよび所定の複数のアクセスキーが記憶された記憶部と、この記憶部に記憶された前記複数のアクセスキーのうちの一つを選択してデータ交換相手である利用者の前記カード型無線端末との間で無線でやりとりする無線通信部と、この無線通信部によって前記他のカード型無線端末より受信したアクセスキーを前記記憶部に外部アクセスキーとして登録する外部アクセスキー登録手段と、前記コンピュータとのインタフェース部とを有し、前記サーバが、前記各利用者の交換対象データが格納されるデータ格納スペースと、一方の利用者の前記コンピュータよりインターネットを通じて転送された個々の交換対象データを前記一方の利用者の前記カード型無線端末の前記記憶部に記憶された個々の前記アクセスキーで各々暗号化して前記データ格納スペースに格納する機能と、他方の利用者の前記コンピュータよりインターネットを通じて転送された、該他方の利用者の前記カード型無線端末の前記記憶部に登録された前記外部アクセスキーに基づいて前記データ格納スペースより前記一方の利用者の交換対象データを取り出して前記外部アクセスキーにより復号し、かつ復号された交換対象データを前記他方の利用者の前記カード型無線端末の前記記憶部に記憶された前記カードIDにより暗号化して該他方の利用者の前記コンピュータへ配信する配信機能とを有し、かつ前記カード型無線端末がそれぞれ、前記サーバより配信された交換対象データを前記記憶部に記憶され

た前記カードIDで復号する機能をさらに有することを特徴とする。

【0017】すなわち、この発明では、異なる内容の複数の交換対象データをそれぞれ異なるアクセスキーで暗号化してサーバのデータ格納スペースに配置しておき、配信相手に応じて公開してよい交換対象データの暗号化に用いた一つのアクセスキーを各カード型無線端末を通じて配信相手に通知する。したがって、本発明によれば、前記第1の発明および第2の発明と同様の作用効果が奏せられるとともに、配信相手によって公開する交換対象データを選択できることによって実用性の高いデータ交換システムを提供することができる。

【0018】さらに第4の発明のパスワード処理方法は、少なくともカードIDを記憶する記憶部と、この記憶部に記憶されたカードIDで暗号化データを復号する復号部と、コンピュータとのインタフェース部とを備えたカード型パスワード記憶装置をコンピュータに接続しておくとともに、前記コンピュータをこのコンピュータ上で動作されるソフトウェアの使用制限を解除するためのパスワードを保持するサーバとインターネットを通じて接続しておき、前記コンピュータは前記サーバに前記カード型パスワード記憶装置の前記記憶部に記憶されたカードIDを転送し、前記サーバは前記コンピュータから転送されたカードIDで前記パスワードを暗号化して前記コンピュータに送信し、前記カード型パスワード記憶装置は前記コンピュータ経由で前記暗号化されたパスワードを取り込んで前記記憶部に登録し、前記コンピュータ上で前記ソフトウェアが起動される度に、前記記憶した暗号化パスワードを前記記憶部に記憶されたカードIDで復号して前記コンピュータへ転送することを特徴とする。

【0019】本発明によれば、インターネット上でパスワードをカードIDで暗号化したかたちで配信することで、ソフトウェア提供者と利用者との間でパスワードを安全にやりとりすることが可能になるとともに、利用者が直接パスワードを参照することができないために、パスワードの漏洩も防止することができる。

【0020】

【発明の実施の形態】以下、本発明を実施する場合の形態について図面を参照して説明する。図1は、本発明の一実施形態である個人データ交換システムの全体的な構成を示す図である。

【0021】図1において、1はWebサーバであり、このWebサーバ1には同システムを利用可能な個々のユーザ専用のデータ格納スペース1-1、1-2を有している。

【0022】2は同システムを利用可能なA氏のコンピュータであり、Webサーバ1とインターネットを通じて接続されている。A氏は自身のコンピュータ2からWebサーバ1上の自分のデータ格納スペース1-1にデ

ータここではA氏の詳細個人データなどを配置することが許されている。

【0023】3は同じく同システムを利用可能なB氏のコンピュータであり、Webサーバ1とインターネットを通じて接続されている。B氏も同様に自身のコンピュータ3からWebサーバ1上の自分のデータ格納スペース1-2にB氏の詳細個人データなどを配置することが許されている。

【0024】さらに、各ユーザは、所定の手続きによって他者の詳細個人データをWebサーバ1からダウンロードすることが許されている。

【0025】4はA氏が利用するカード型無線端末、5は同じくB氏が利用するカード型無線端末である。これらのカード型無線端末4、5は相互に無線でデータを送受信することが可能である。

【0026】図2に、このカード型無線端末の外観を示す。このカード型無線端末4(5)は名刺程度のサイズを持ち、主面には文字や画像を表示する液晶ディスプレイ等の表示器11と、各種の音声出力するスピーカ12と、通信状態などを発光によりユーザに通知するLED13と、表示をスクロール操作するためのスクロールボタン14と、ユーザから通信開始の指示を与えるための通信ボタン15とが設けられている。

【0027】さらに、カード型無線端末4(5)の側面には、コンピュータ2(3)との光通信用のI/Oポート16と、電源のオン・オフを切り替える電源スイッチ17と、他のカード型無線端末との間でたとえば赤外線信号などの無線信号を送受信する無線通信部18とが設けられている。

【0028】また、このカード型無線端末4(5)には、全体の制御ならびにデータの処理を行うMPUと不揮発性のメモリ部とが少なくとも内蔵されている。メモリ部には、図3に示すように、制御用のプログラム、カードIDなどが固定的に格納される予約エリア31の他、本人のアクセスキー、本人の詳細個人データが置かれているWebサーバ1上の場所を示すURLを少なくとも含む簡易個人データ、さらには他者のカード型無線端末から取得し、本人のカードIDによって暗号化したデータなどが記憶されるユーザエリア32が設けられている。

【0029】アクセスキーとは、Webサーバ1上に置いた詳細個人データをアクセスするために必要なキーである。Webサーバ1上に詳細個人データが格納される際にはその詳細個人データを前記のアクセスキーで暗号化し、逆にWebサーバ1から詳細個人データを読み出す際には暗号化された詳細個人データを同一のアクセスキーで復号するようにしている。これにより、Webサーバ1上に置かれた詳細個人データの改ざん防止を図っている。

【0030】次に、本実施形態の個人データ交換システ

ムにおける動作の例として、A氏からB氏へ、A氏の詳細個人データを配信する場合の動作を説明する。図4に、A氏が自分の詳細個人データをWebサーバ1にアップロードする時の流れを示す。

【0031】ステップ401で、まずA氏は自分のコンピュータ2上で自分の詳細個人データを作成する。詳細個人データの内容は目的に応じてA氏が自由に決めることができる。たとえば名刺の交換や自己PRの場として本システムを利用する場合、本人の氏名、連絡先、勤め先、電話番号、電子メールアドレス、経歴、趣味などを詳細個人データとすることができる。

【0032】次に、A氏が自分のコンピュータ2をWebサーバ1にインターネットを通じて接続すると、Webサーバ1からカードIDが要求される。そこでステップ402で、この要求に対してコンピュータ2はA氏のカード型無線端末4のカードIDをWebサーバ1に転送する。

【0033】この処理は、予めA氏のコンピュータ2にWebサーバ1からの要求に対して応答すべきカードIDを予め設定しておくことで、Webサーバ1からの要求に応じてカードIDの送信を自動で行うようにすることが可能である。また、カード型無線端末4とコンピュータ2とを接続しておき、カード型無線端末4に記憶されたカードIDをコンピュータ2を経由してWebサーバ1へ送るようにしてもよい。あるいは、ユーザ自身がコンピュータ2からカードIDを手入力してもよい。

【0034】ステップ403では、Webサーバ1上で、A氏から応答されたカードIDと予めWebサーバ1に登録済みの正規ユーザのカードIDとの照合による認証が行われる。この認証に失敗した場合はステップ404でエラーにより処理は終了される。

【0035】ステップ405では、コンピュータ2上で作成しておいたA氏の詳細個人データをWebサーバ1に転送する。これによりWebサーバ1の一次記憶領域にA氏の詳細個人データが保持される。

【0036】ステップ406で、カード型無線端末4に登録されたA氏のアクセスキーをWebサーバ1に送信する。この処理は、カードIDの場合と同様に、予めA氏のコンピュータ2にWebサーバ1からの要求に対して応答すべきA氏のアクセスキーを予め設定しておくことで、Webサーバ1からの要求に応じてアクセスキーの転送を自動で行うようにすることが可能である。また、カード型無線端末4とコンピュータ2とを接続しておき、カード型無線端末4に記憶されたアクセスキーをコンピュータ2を経由してWebサーバ1へ送るようにしてもよい。あるいは、ユーザ自身がコンピュータ2からアクセスキーを手入力してもよい。

【0037】ステップ407では、Webサーバ1は、一次記憶領域に保持されたA氏の詳細個人データを同じくA氏から送られてきたアクセスキーにより暗号化する

処理が行われる。こうして暗号化されたA氏の詳細個人データは、ステップ408で、Webサーバ1のA氏用のデータ格納スペース1-1に保存される。

【0038】ステップ409で、A氏は当該詳細個人データに再配信防止の属性を付与するかどうかを選択する。ステップ410で、その再配信防止の属性の選択結果がWebサーバ1に保持される。

【0039】A氏は、以上のようなWebサーバ1への詳細個人データのアップロードを行った後、B氏との間でカード型無線端末4、5による以下のようなデータ交換を行う。

【0040】すなわち、A氏はWebサーバ1に置いてある自分の詳細個人データをB氏に公開するため、A氏のカード型無線端末4からB氏のカード型無線端末5へ、A氏のカード型無線端末4のメモリ部に記憶してある、アクセスキーならびにURLを含む簡易個人データを無線送信し、B氏のカード型無線端末5のメモリ部に記憶させる。このときA氏の簡易個人データは、B氏のカードIDによって暗号化されて記憶される。

【0041】次に、B氏がWebサーバ1上のA氏の詳細個人データにアクセスしてコンピュータ3上で閲覧する場合の動作を説明する。図5に、かかるB氏によるA氏の詳細個人データの取得の流れを示す。

【0042】B氏は既にA氏からアクセスキーと詳細個人データの置き場所を示すURLを含む簡易個人データを取得しており、まず、ステップ501で、自分のコンピュータ3をWebサーバ1にインターネットを通じて接続し、Webサーバ1にA氏から取得したアクセスキー（以下、外部アクセスキーと呼ぶ）とURLを送信する。

【0043】この際、予めコンピュータ3に外部アクセスキーとURLとを登録しておくことで、Webサーバ1への外部アクセスキーの送信を自動で行うようにすることが可能である。また、カード型無線端末5とコンピュータ3とを接続しておき、カード型無線端末5に保持された外部アクセスキーとURLをコンピュータ3を経由してWebサーバ1へ送るようにしてもよい。あるいは、ユーザがカード型無線端末5の表示画面で外部アクセスキーとURLを確認しておき、コンピュータ3から外部アクセスキーとURLとを手入力してもよい。

【0044】次に、ステップ502では、Webサーバ1上で、B氏から送られてきた外部アクセスキーと、この外部アクセスキーとともに送られてきたURLが示すWebサーバ1上の詳細個人データの暗号化に使用されたアクセスキーとの照合によるアクセス権の有無の判定が行われる。双方のアクセスキーが不一致の場合はアクセス権が無いものと判定され、詳細個人データを取得する処理は途中終了になる（ステップ503）。

【0045】双方のアクセスキーが一致した場合、ステップ504でWebサーバ1はA氏用のデータ格納ス

10

20

30

40

50

ース1-1から該当する詳細個人データを取り出す。

【0046】ステップ505で、Webサーバ1は取り出した詳細個人データに再配信防止の属性が付与されているかどうかを調べる。再配信防止の属性が付与されていなければ、ステップ506で、Webサーバ1は当該詳細個人データをB氏から送られてきた外部アクセスキーで復号してB氏のコンピュータ3へ送信する。

【0047】これによりステップ507で、Webサーバ1からダウンロードされたA氏の詳細個人データがB氏のコンピュータ3上で閲覧される。B氏のコンピュータ3に取り込まれたA氏の詳細個人データは、ステップ508で、住所録作成、携帯電話配信などの二次利用に供される。

【0048】一方、ステップ505で、詳細個人データに再配信防止の属性が付与されていた場合、Webサーバ1は、ステップ509で、A氏の詳細個人データをB氏から送られてきた外部アクセスキーで復号する。

【0049】次に、ステップ510で、Webサーバ1は、B氏のコンピュータ3に対してB氏のカード型無線端末5に登録されているカードIDの取得を要求する。B氏のコンピュータ3は、この要求に対してカードIDを応答する。

【0050】この処理は、予めB氏のコンピュータ3にWebサーバ1からの要求に対してカードIDを応答するように設定しておくことで、Webサーバ1へのカードIDの送信を自動で行うようにすることが可能である。また、カード型無線端末5とコンピュータ3とを接続しておき、カード型無線端末5に保持されたカードIDをコンピュータ3を経由してWebサーバ1へ送るようにしてもよい。あるいは、ユーザがコンピュータ3からカードIDを手入力してもよい。

【0051】続いて、ステップ511でWebサーバ1は、取得したB氏のカードIDによりA氏の詳細個人データを暗号化してB氏のコンピュータ3へ送信する。ステップ512では、B氏のコンピュータ3が、Webサーバ1よりダウンロードしたA氏の詳細個人データをB氏のカードIDにより復号する。

【0052】これによりステップ507で、Webサーバ1からダウンロードされたA氏の詳細個人データがB氏のコンピュータ3上で閲覧される。B氏のコンピュータ3に取り込まれたA氏の詳細個人データは、ステップ508で、住所録作成、携帯電話配信などの二次利用に供される。

【0053】以上説明した通り、本実施形態は次のような特長をもつ。インターネットを利用した詳細個人データのやりとりにおいて、個人どうしが直接面会した際に両者が所持しているカード型無線端末間での無線による小容量の簡易個人データの交換を行い、カード型無線端末に取り込んだ簡易個人データを使ってWebサーバ1上のより大容量の詳細個人データにアクセスしてその内

容を参照することができる。すなわち、直接面会した相手だけに詳細個人データの公開先を制限することができる、セキュリティの向上を図ることができる。

【0054】また、詳細個人データをWebサーバ1上に配置したユーザは当該詳細個人データに再配信防止の属性を付与できる。この属性の付与された詳細個人データは、配信相手のカードIDによって暗号化されて送信されるので、ダウンロード先のコンピュータから外部へ再配信されたとしても、再配信先では詳細個人データを復号して中身を参照することはできない。したがって、個人データの漏洩を防止でき、セキュリティを強化できる。

【0055】次に、第2の実施形態を説明する。本実施形態は複数のアクセスキーに関するものである。

【0056】前提とするシステムの全体構成及びカード型無線端末の構成は前記の実施形態と同様であるが、本実施形態は、自分の詳細個人データを複数用意し、それぞれの詳細個人データを異なるアクセスキーで暗号化してWebサーバ1の自分のデータ格納スペース1-1に配置できるようにした点に特徴がある。

【0057】図6に、本実施形態の個人データ交換システムの全体的な構成を示す。同図において、61はA氏のカード型無線端末4のメモリ部における簡易個人データの例であり、ここには、A氏の仕事用のアクセスキーA1およびURLと、プライベート用のアクセスキーA2およびURLが記憶されている。ここで、仕事用のURLは、Webサーバ1上のA氏のデータ格納スペース1-1に配置した仕事用の詳細個人データの格納位置1-11を指し、プライベート用のURLは、同じくA氏のデータ格納スペース1-1に配置したプライベート用の詳細個人データの格納位置1-12を指す。

【0058】状況として、A氏が仕事上C氏へ自分の詳細個人データを公開する場合が生じたものとする。ただしC氏はカード型無線端末を利用しておらず、C氏はインターネットに接続可能なコンピュータ6を持っているとする。

【0059】この場合、A氏は、カード型無線端末4の通信ポート16を通じて無線でC氏のコンピュータ6へ自分の仕事用のアクセスキーA1およびURLを転送する。C氏は、自分のコンピュータ6をWebサーバ1にインターネットを通じて接続し、A氏のカード型無線端末4から取得したアクセスキーA1およびURLをWebサーバ1に送信する。この結果、Webサーバ1は、A氏のデータ格納スペース1-1からURLが指す仕事用の詳細個人データ1-11を取り出し、アクセスキーA1で復号後、C氏のコンピュータ6に送信する。

【0060】また、B氏はA氏とプライベートな関係を持ち、カード型無線端末5を利用しているものとする。

【0061】したがって、A氏はB氏にカード型無線端末4(5)による無線通信でプライベート用のアクセス

10

20

30

40

50

キー A 2 および URL を提供する。A 氏は、自分のコンピュータ 2 を Web サーバ 1 にインターネットを通じて接続し、A 氏のカード型無線端末 4 から取得したアクセスキー A 2 および URL を Web サーバ 1 に送信する。この結果、Web サーバ 1 は、A 氏のデータ格納スペース 1-1 から URL が指すプライベート用の詳細個人データ 1-12 を取り出し、アクセスキー A 2 で復号後、たとえば B 氏のカード ID で暗号化を行った後、B 氏のコンピュータ 5 に送信する。

【0062】したがって、本実施形態によれば、複数のアクセスキーと異なる詳細個人データを用意しておく、相手によって異なるアクセスキーを提供しておくことで、相手によって異なる内容の詳細個人データを配信することが可能になる。

【0063】次に、本発明に係る第 3 の実施形態であるカード型パスワード処理装置について説明する。

【0064】このカード型パスワード処理装置は、コンピュータ上で動作されるビデオ、音楽、ゲーム、アプリケーションプログラム等の著作権情報であるソフトウェアに対してソフトウェア提供者が設けた使用制限を解除するためのパスワードをコンピュータへ提供するための手段として利用される。

【0065】図 7 において、8 はソフトウェア提供者が提供しているソフトウェアの使用制限を解除するためのパスワード A、B をインターネットを通じて各クライアントのコンピュータへ提供するサーバ、10 はソフトウェア提供者が提供するソフトウェアを利用するコンピュータ、9 はカード型パスワード処理装置である。

【0066】カード型パスワード処理装置 9 は、記憶部 71 に少なくともカード ID 82 を記憶している。コンピュータ 10 とは I/O ポート 72 を通じて接続可能とされ、この I/O ポート 72 を通じてサーバ 8 から配信された暗号化パスワード 83 (84) がコンピュータ 10 を経由して記憶部 71 に登録されるようになっている。また、カード型パスワード処理装置 9 は、コンピュータ 10 上でソフトウェアが起動される際にコンピュータ 10 からパスワードの入力依頼を受け、この依頼に応じて記憶部 71 から暗号化パスワード 83 (84) を読み出し、復号部 73 にて、当該暗号化パスワード 83 (84) をカード ID で復号してコンピュータ 10 に転送するように構成されている。

【0067】以下に、この処理を詳しく説明する。まずコンピュータ 10 からソフトウェア提供者のサーバ 8 に向けてたとえばパスワード A の取得を要求したとする。この際、カード型パスワード処理装置 9 の記憶部 71 に記憶されたカード ID 82 をソフトウェア提供者のサーバ 8 に転送する。サーバ 8 は取得したカード ID 82 で当該ソフトウェアのパスワード A を暗号化してコンピュータ 10 へ配信する。サーバ 8 から送信された暗号化パスワード 83 はコンピュータ 10 を経由してカード型パ

スワード処理装置 9 に取り込まれ、記憶部 71 に登録される。

【0068】この後、カード型パスワード処理装置 9 は、コンピュータ 10 上でソフトウェアが起動される度に発行されるパスワード入力依頼を従って記憶部 71 に登録された暗号化パスワード 83 をカード ID 82 で復号してコンピュータ 10 に転送する。

【0069】したがって、本実施形態によれば、インターネット上でパスワードをカード ID で暗号化したかたちで配信することで、ソフトウェア提供者と利用者との間でパスワードを安全にやりとりすることが可能になるとともに、利用者が直接パスワードを参照することができないために、パスワードの漏洩も防止することができる。

【0070】次に、本発明の第 4 の実施形態を説明する。本実施形態は、カード型無線端末を電子商取引に用いたものである。

【0071】図 8 に本実施形態の全体的なシステム構成を示す。同図において、A 氏と D 氏との間でカード型無線端末 4、94 を使って電子マネーをやりとり場合、双方のカード型無線端末 4、94 の間で互いのカード ID を取引金額などの取引データとともにやりとりしてメモリ部に記憶する。この後、A 氏、D 氏の各々のコンピュータ 2、91 において Web サーバ 101 との間で以下のやりとりが行われる。

【0072】A 氏は自分のコンピュータ 2 をインターネットを通じて Web サーバ 101 に接続し、A 氏のカード ID と暗証番号等による本人認証を受ける。この際、たとえば、カード ID はカード型無線端末 4 をコンピュータ 2 に接続しておき、カード型無線端末 4 からコンピュータ 2 がカード ID を読み出して Web サーバ 101 に与えられ、暗証番号はたとえばコンピュータ 2 上で A 氏自身が手入力することによって Web サーバ 101 に与えられる。なお、この処理には様々な変形があり、上記方法に限定されない。一方、D 氏の側においても同様に本人認証が行われる。

【0073】A 氏、D 氏ともに本人認証に成功すれば、続いて A 氏、D 氏の双方において、自分のカード ID、取引相手のカード ID、取引データなどの、取引を特定するために必要なデータが Web サーバ 101 に転送される。

【0074】Web サーバ 101 は A 氏、D 氏の双方から転送された情報を照合し、一致する場合は取引内容を示すデータに従って A 氏と D 氏との間での電子決済を実行する。

【0075】また、本人認証が成功した後であれば、自分の口座残高、決済内容をダウンロードしてコンピュータ上で閲覧することが可能である。

【0076】この決済方法の特長の一つは、カード型無線端末が既知のクレジットカードのような取扱いで気軽

19

に利用できるという点のみならず、カード型無線端末間の無線通信によって、カード型無線端末は一切本人から手放されることなくデータのやりとりを行えるという点にある。したがって、より安全な電子決済が可能になる。

【0077】

【発明の効果】以上、説明したように本発明のデータ交換システム、データ交換方法およびカード型無線端末によれば、配信を受ける側の利用者は、データを提供する側の利用者のカード型無線端末からアクセスキーをもらい受けてはじめて交換対象データの配信を受けることが可能となるので、データを交換する当事者どうしが直接面会したことを条件としたデータ交換が可能となり、セキュリティの向上を図ることができる。

【0078】また、本発明のデータ交換システム、データ交換方法およびカード型無線端末によれば、サーバから配信先のコンピュータへ、交換対象データが当該配信先の利用者のカード型無線端末のカードIDによって暗号化されて配信されるので、仮に配信先のコンピュータから交換対象データが外部へ再配信されたとしても、再配信先では前記カードIDによる暗号化データを復号して中身を参照することはできない。したがって、個人情報の漏洩を防止でき、セキュリティを強化できる。

【0079】さらに、本発明のデータ交換システム、データ交換方法およびカード型無線端末によれば、配信相手によって公開する交換対象データを選択できることによって実用性の高いデータ交換システムを提供することができる。

【0080】さらに、本発明のパスワード処理方法およびカード型パスワード処理装置によれば、インターネット上でパスワードをカードIDで暗号化したかたちで配

(11)

特開2002-281012

20

信することで、ソフトウェア提供者と利用者との間でパスワードを安全にやりとりすることが可能になるとともに、利用者が直接パスワードを参照することができないために、パスワードの漏洩も防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態である個人データ交換システムの全体的な構成を示す図である。

【図2】図1におけるカード型無線端末の外観図である。

10 【図3】図2のカード型無線端末のメモリ部の構成を示す図である。

【図4】詳細個人データをWebサーバにアップロードする時の流れを示す図である。

【図5】Webサーバから詳細個人データを取得する場合の流れを示す図である。

【図6】本発明の第2の実施形態の個人データ交換システムの全体的な構成を示す図である。

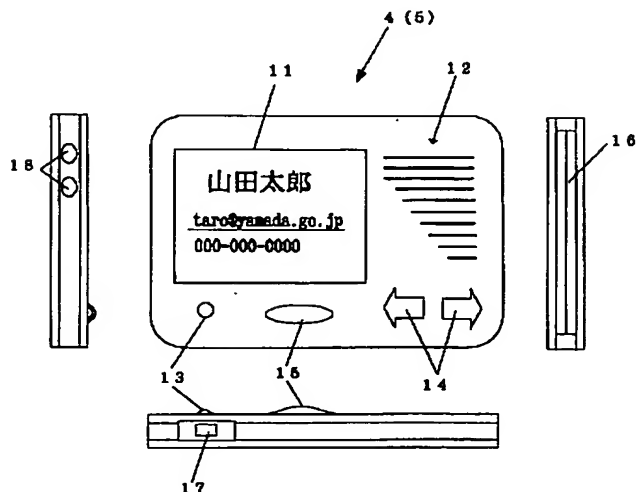
【図7】本発明の第3の実施形態であるカード型パスワード処理装置を説明するための図である。

20 【図8】本発明の第4の実施形態であるカード型無線端末を用いた電子商取引システムの全体的な構成を示す図である。

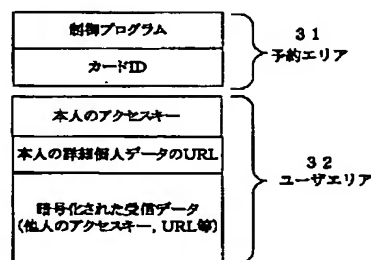
【符号の説明】

1…Webサーバ 1-1, 1-2…データ格納スペース 2, 3, 5, 6, 10, 91…コンピュータ 4, 5, 94…カード型無線端末 8…サーバ 9…カード型パスワード処理装置 11…表示器 16…通信ポート 18…無線通信部 71…記憶部 73…復号部 83…暗号化パスワード

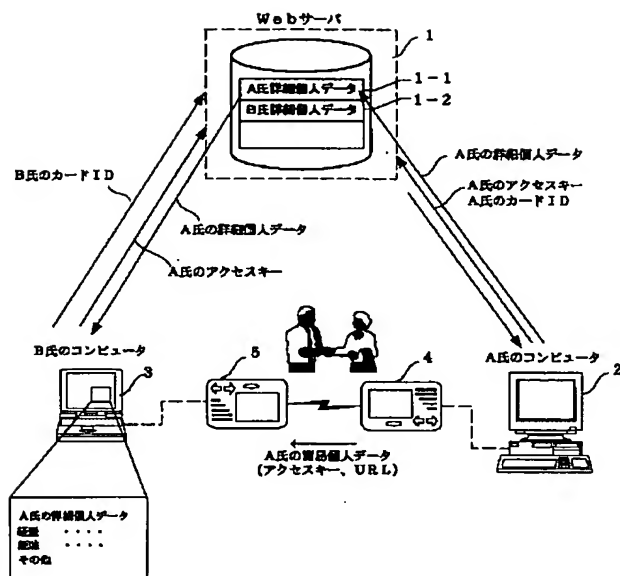
【図2】



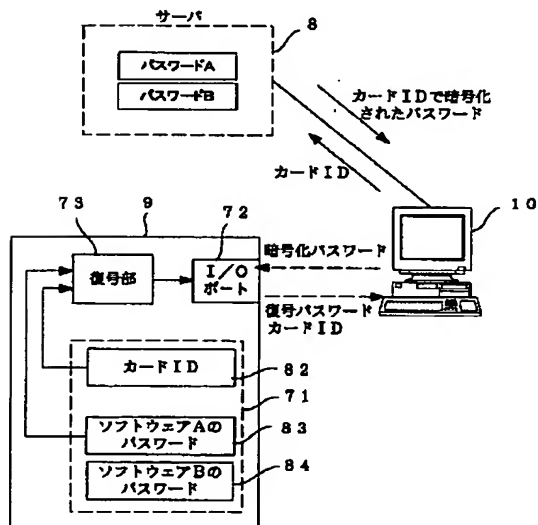
【図3】



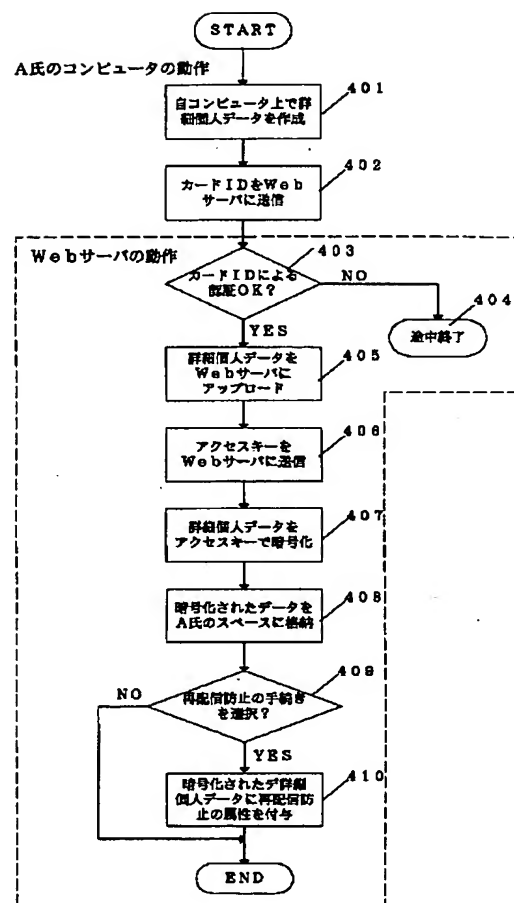
【図 1】



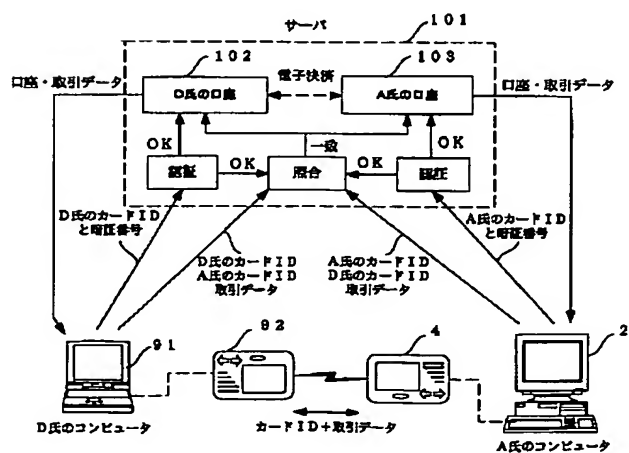
【図 7】



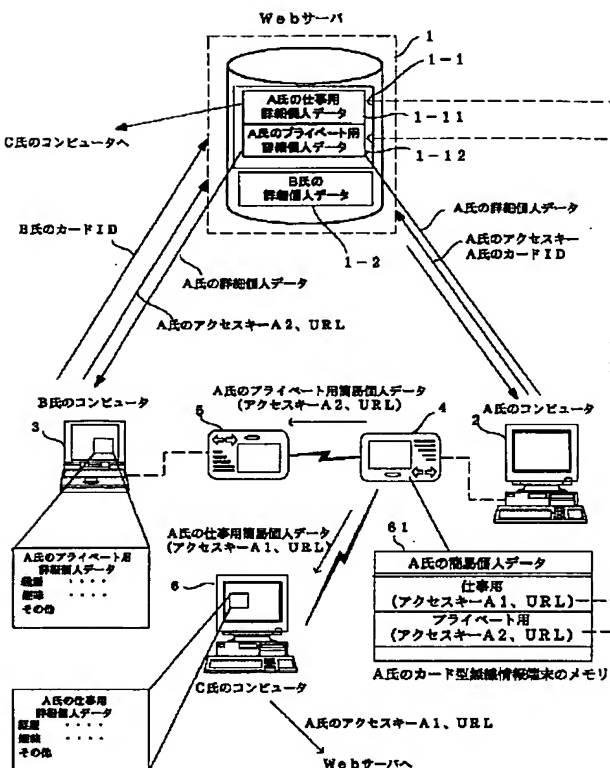
【図 4】



【図 8】



【図 6】



(72) 発明者 宮内 健
東京都青梅市新町 3 丁目 3 番地の 1 東芝
デジタルメディアエンジニアリング株式会
社内

(72) 発明者 木村 太司
東京都青梅市新町 3 丁目 3 番地の 1 東芝
デジタルメディアエンジニアリング株式会
社内

Fターム(参考) 5B085 AA08 AE01 AE29
5J104 AA01 AA07 AA16 EA03 EA04
EA26 KA02 NA02 NA36 NA37
NA38 PA09 PA14